PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-010044
(43)Date of publication of application : 11.01.2002

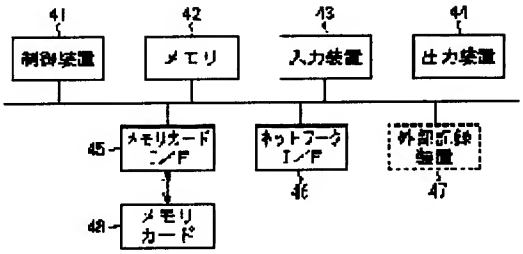
(51)Int.Cl. H04N 1/21
G06F 3/06
G06F 3/08
G06K 19/10
G06K 19/07
// H04L 9/32

(21)Application number : 2000-184993
(22)Date of filing : 20.06.2000

(71)Applicant : CANON INC
(72)Inventor : KASAI KAZUHIRO

(54) MEMORY CARD, DEVICE AND METHOD FOR FORMING IMAGE, AND STORAGE MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To improve the reliability of image file data by preventing alteration in the image file data that is created by an image-forming device for storing into a memory card.
SOLUTION: When the image file data that is created by the image-forming device is to be stored into the memory card, a unidirectional function is used for calculating the message digest value of the image file data, a secret key is used for signing the message digest value, and the signature is stored into the memory card with the image file data, thus preventing the signature from being easily altered for improving the reliability of the image file data.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2002－10044
（P2002－10044A）
(43)公開日　平成14年１月11日(2002.1.11)

(51)Int.Cl.'		識別記号	FI		テーマコード'(参考)
H04N	1/21		H04N	1/21	5B035
G06F	3/06	304	G06F	3/06	304H 5B065
	3/08			3/08	C 5C073
G06K	19/10		G06K	19/00	R 5J104
	19/07				N

審査請求　未請求　請求項の数21　ＯＬ　（全 12 頁）　最終頁に続く

(21)出願番号　特願2000－184993(P2000－184993)

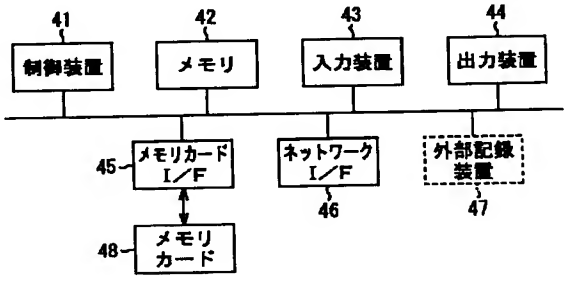
(22)出願日　平成12年６月20日(2000.6.20)

(71)出願人　000001007
キヤノン株式会社
東京都大田区下丸子３丁目30番２号
(72)発明者　笠井　一宏
東京都大田区下丸子３丁目30番２号　キヤノン株式会社内
(74)代理人　100090273
弁理士　國分　孝悦

Ｆターム(参考)　5B035 AA13 BB09 BC00 CA38
5B065 BA09 PA13 PA20
5C073 AA03 AA06 AB04 AB05 CE04
CE10
5J104 AA09 LA03 LA05 LA06 NA02
NA33 PA14

(54)【発明の名称】　メモリカード、画像形成装置、画像形成方法及び記憶媒体

(57)【要約】
【課題】　画像形成装置で作成してメモリカードに保存されている画像ファイルデータの改ざんを防止して、前記画像ファイルデータの信頼性を向上させる。
【解決手段】　画像形成装置で作成した画像ファイルデータをメモリカードに保存する際に、一方向性関数を用いて前記画像ファイルデータのメッセージダイジェスト値を算出し、秘密鍵を用いて前記メッセージダイジェスト値を署名し、前記署名を前記画像ファイルデータと一緒に前記メモリカードに保存することにより、署名の改ざんを行い難くして前記画像ファイルデータの信頼性を向上できるようにする。



1

【特許請求の範囲】

【請求項１】　画像形成装置により作成された画像ファイルデータの電子署名を記録可能な領域を有するメモリカードであって、

前記画像形成装置以外による書き込みを禁止するように設定可能なデータ記憶領域が形成され、前記データ記憶領域に前記電子署名が記録されるようになされていることを特徴とするメモリカード。

【請求項２】　画像形成装置により作成された画像ファイルデータに電子署名を施す際に使用する秘密鍵と、前記秘密鍵と対となる公開鍵とを記録可能な領域を有するメモリカードであって、

前記画像形成装置以外による書き込みを禁止するように設定可能なデータ記憶領域が形成され、前記データ記憶領域に前記秘密鍵及び公開鍵が記録されるようになされていることを特徴とするメモリカード。

【請求項３】　機器固有の秘密鍵を保持し、前記機器固有の秘密鍵を用いて電子署名を施すことを特徴とする画像形成装置。

【請求項４】　ユーザ定義による秘密鍵を新規に作成する秘密鍵作成手段を具備し、前記秘密鍵作成手段で作成した秘密鍵を用いて電子署名を施すことを特徴とする画像形成装置。

【請求項５】　メモリカードにアクセス可能なインターフェースを備えた画像形成装置において、

前記メモリカード内のプロパティファイル領域に機器固有の秘密鍵もしくはユーザ定義による秘密鍵を保存する鍵保存手段を有することを特徴とする画像形成装置。

【請求項６】　前記機器固有の秘密鍵もしくはユーザ定義による秘密鍵を表示装置上に可視的に表示する鍵情報表示制御手段を有することを特徴とする請求項５に記載の画像形成装置。

【請求項７】　前記機器固有の秘密鍵と対となる機器固有の公開鍵を保有することを特徴とする請求項５または６に記載の画像形成装置。

【請求項８】　前記ユーザ定義による秘密鍵と対となるユーザ定義による公開鍵を作成する公開鍵作成手段を有することを特徴とする請求項５～７の何れか１項に記載の画像形成装置。

【請求項９】　所定の画像形成装置以外による書き込みを禁止するように設定可能なデータ記憶領域が形成され、前記データ記憶領域に電子署名が記録されるようになされているメモリカードにアクセス可能なインターフェースを備えた画像形成装置において、

前記メモリカード内のプロパティファイルに、機器固有の公開鍵もしくは前記ユーザ定義による公開鍵の情報を保存する鍵情報保存手段を有することを特徴とする画像形成装置。

【請求項１０】　前記機器固有の公開鍵もしくはユーザ定義による公開鍵を表示装置上に可視的に表示する鍵情報表示制御手段を有することを特徴とする請求項９に記載の画像形成装置。

2

【請求項１１】　作成した画像ファイルデータをメモリカードに保存するデータ保存手段を有する画像形成装置であって、

前記画像ファイルデータに対して一方向性関数を用いて前記画像ファイルデータに固有のメッセージダイジェスト値を算出する算出手段と、

前記メッセージダイジェスト値を前記機器固有の秘密鍵もしくはユーザ定義による秘密鍵により暗号化して署名を得る署名手段と、

前記署名をメモリカード内のプロパティ領域に保存するとともに、署名対象の画像ファイルデータをメモリカード内の画像ファイル領域に保存する保存手段とを有することを特徴とする画像形成装置。

【請求項１２】　ユーザ定義による秘密鍵を新規に作成する秘密鍵作成処理を行ない、前記秘密鍵作成処理で作成した秘密鍵を用いて電子署名を施すことを特徴とする画像形成方法。

【請求項１３】　メモリカードにアクセス可能なインターフェースを備えた装置を用いた画像形成方法において、

前記メモリカード内のプロパティファイル領域に機器固有の秘密鍵もしくはユーザ定義による秘密鍵を保存する鍵保存処理を行うことを特徴とする画像形成方法。

【請求項１４】　前記機器固有の秘密鍵もしくはユーザ定義による秘密鍵を表示装置上に可視的に表示する鍵情報表示制御処理を行うことを特徴とする請求項１３に記載の画像形成方法。

【請求項１５】　前記機器固有の秘密鍵と対となる機器固有の公開鍵を使用して電子署名を施すことを特徴とする請求項１３または１４に記載の画像形成方法。

【請求項１６】　前記ユーザ定義による秘密鍵と対となるユーザ定義による公開鍵を作成する公開鍵作成処理を行うことを特徴とする請求項１３～１５の何れか１項に記載の画像形成方法。

【請求項１７】　メモリカードにアクセス可能なインターフェースを備えた装置を用いた画像形成方法において、

前記メモリカード内のプロパティファイルに、機器固有の公開鍵もしくはユーザ定義による公開鍵を保存する鍵情報保存処理を行うことを特徴とする画像形成方法。

【請求項１８】　前記機器固有の公開鍵もしくはユーザ定義による公開鍵を表示装置上に可視的に表示する表示制御処理を行うことを特徴とする請求項１７に記載の画像形成方法。

【請求項１９】　作成した画像ファイルデータをメモリカードに保存するデータ保存処理を行う画像形成方法であって、

前記画像ファイルデータに対して一方向性関数を用いて

前記画像ファイルデータに固有のメッセージダイジェスト値を算出する算出処理と、
前記メッセージダイジェスト値を前記機器固有の秘密鍵もしくはユーザ定義による秘密鍵により暗号化して署名を得る署名処理と、
前記署名をメモリカード内のプロパティ領域に保存するとともに、署名対象の画像ファイルデータをメモリカード内の画像ファイル領域に保存する保存処理とを行うことを特徴とする画像形成方法。
【請求項２０】　前記請求項１～１１の何れかに記載の各手段を構成するプログラムをコンピュータから読み出し可能に格納したことを特徴とする記憶媒体。
【請求項２１】　前記請求項１２～１９の何れか１項に記載の画像形成方法を実行するプログラムをコンピュータから読み出し可能に格納したことを特徴とする記憶媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明はメモリカード、画像形成装置、画像形成方法及び記憶媒体に関し、特に、画像ファイルデータの改ざんを防止するために用いて好適なものである。
【０００２】
【従来の技術】従来、電子スチルカメラなどといった画像形成装置で作成した画像ファイルデータをメモリカードに保存する方法が行われている。前記メモリカードを用いて前記画像ファイルデータを印刷する場合であれば、プリンタと接続されたパーソナルコンピュータ（以下、ＰＣと省略）もしくはプリンタ自体に、前記メモリカードにアクセス可能なインターフェース（以下、Ｉ／Ｆと省略）を備えれば、前記メモリカードを接続することによりプリントすることができる。
【０００３】また、前記画像ファイルデータをパーソナルコンピュータ、あるいは電子手帳等に転送する場合であれば、メモリカードへアクセス可能なＩ／Ｆを備えた被転送装置に前記メモリカードを接続することにより、画像ファイルデータの授受を容易に行うことができる。
【０００４】
【発明が解決しようとする課題】しかし、前記従来例の保存方法においては、以下のような問題があった。すなわち、メモリカード内に保存されている画像ファイルデータは電子的なデータであるため複製が容易である。そのために、不正複製、不正利用、改ざん等が行われる問題があった。したがって、前記メモリカードに保存されている画像ファイルデータが改ざんされたものではなく、正当なデータであることを証明する必要が出てきた。
【０００５】そこで、本発明は画像形成装置にて画像ファイルデータをメモリカードに保存する際に、保存対象の画像ファイルデータに電子署名を施すことで、前記画像ファイルデータの信頼性を向上させることを目的とする。

【０００６】また、前記画像形成装置以外による書き込みを禁止するように設定可能なデータ記憶領域に前記電子署名を記録することで、信頼性さらにを向上させることを目的とする。
【０００７】また本発明は、メモリカード内に格納する画像ファイルデータの改ざんを防止し、そのデータの信頼性を向上させることを目的としている。
【０００８】
【課題を解決するための手段】本発明のメモリカードは、画像形成装置により作成された画像ファイルデータの電子署名を記録可能な領域を有するメモリカードであって、前記画像形成装置以外による書き込みを禁止するように設定可能なデータ記憶領域が形成され、前記データ記憶領域に前記電子署名が記録されるようになされていることを特徴としている。また、本発明の他の特徴とするところは、画像形成装置により作成された画像ファイルデータに電子署名を施す際に使用する秘密鍵と、前記秘密鍵と対となる公開鍵とを記録可能な領域を有するメモリカードであって、前記画像形成装置以外による書き込みを禁止するように設定可能なデータ記憶領域が形成され、前記データ記憶領域に前記秘密鍵及び公開鍵が記録されるようになされていることを特徴としている。また、本発明のその他の特徴とするところは、機器固有の秘密鍵を保持し、前記機器固有の秘密鍵を用いて電子署名を施すことを特徴としている。また、本発明のその他の特徴とするところは、ユーザ定義による秘密鍵を新規に作成する秘密鍵作成手段を具備し、前記秘密鍵作成手段で作成した秘密鍵を用いて電子署名を施すことを特徴としている。また、本発明のその他の特徴とするところは、メモリカードにアクセス可能なインターフェースを備えた画像形成装置において、前記メモリカード内のプロパティファイル領域に機器固有の秘密鍵もしくはユーザ定義による秘密鍵を保存する鍵保存手段を有することを特徴としている。また、本発明のその他の特徴とするところは、前記機器固有の秘密鍵もしくはユーザ定義による秘密鍵を表示装置上に可視的に表示する鍵情報表示制御手段を有することを特徴としている。また、本発明のその他の特徴とするところは、前記機器固有の秘密鍵と対となる機器固有の公開鍵を保有することを特徴としている。また、本発明のその他の特徴とするところは、前記ユーザ定義による秘密鍵と対となるユーザ定義による公開鍵を作成する公開鍵作成手段を有することを特徴としている。また、本発明のその他の特徴とするところは、所定の画像形成装置以外による書き込みを禁止するように設定可能なデータ記憶領域が形成され、前記データ記憶領域に電子署名が記録されるようになされているメモリカードにアクセス可能なインターフェースを備えた画像形成装置において、前記メモリカード内のブ

ロバティファイルに、機器固有の公開鍵もしくは前記ユーザ定義による公開鍵の情報を保存する鍵情報保存手段を有することを特徴としている。また、本発明のその他の特徴とするところは、前記機器固有の公開鍵もしくはユーザ定義による公開鍵を表示装置上に可視的に表示する鍵情報表示制御手段を有することを特徴としている。また、本発明のその他の特徴とするところは、作成した画像ファイルデータをメモリカードに保存するデータ保存手段を有する画像形成装置であって、前記画像ファイルデータに対して一方向性関数を用いて前記画像ファイルデータに固有のメッセージダイジェスト値を算出する算出手段と、前記メッセージダイジェスト値を前記機器固有の秘密鍵もしくはユーザ定義による秘密鍵により暗号化して署名を得る署名手段と、前記署名をメモリカード内のプロバティ領域に保存するとともに、署名対象の画像ファイルデータをメモリカード内の画像ファイル領域に保存する保存手段とを有することを特徴としている。

【０００９】本発明の画像形成方法は、ユーザ定義による秘密鍵を新規に作成する秘密鍵作成処理を行ない、前記秘密鍵作成処理で作成した秘密鍵を用いて電子署名を施すことを特徴としている。また、本発明の他の特徴とするところは、メモリカードにアクセス可能なインターフェースを備えた装置を用いた画像形成方法において、前記メモリカード内のプロバティファイル領域に機器固有の秘密鍵もしくはユーザ定義による秘密鍵を保存する鍵保存処理を行うことを特徴としている。また、本発明のその他の特徴とするところは、前記機器固有の秘密鍵もしくはユーザ定義による秘密鍵を表示装置上に可視的に表示する鍵情報表示制御処理を行うことを特徴としている。また、本発明のその他の特徴とするところは、前記機器固有の秘密鍵と対となる機器固有の公開鍵を使用して電子署名を施すことを特徴としている。また、本発明のその他の特徴とするところは、前記ユーザ定義による秘密鍵と対となるユーザ定義による公開鍵を作成する公開鍵作成処理を行うことを特徴としている。また、本発明のその他の特徴とするところは、メモリカードにアクセス可能なインターフェースを備えた装置を用いた画像形成方法において、前記メモリカード内のプロバティファイルに、前記機器固有の公開鍵もしくはユーザ定義による公開鍵を保存する鍵情報保存処理を行うことを特徴としている。また、本発明のその他の特徴とするところは、前記機器固有の公開鍵もしくはユーザ定義による公開鍵を表示装置上に可視的に表示する表示制御処理を行うことを特徴としている。また、本発明のその他の特徴とするところは、作成した画像ファイルデータをメモリカードに保存するデータ保存処理を行う画像形成方法であって、　前記画像ファイルデータに対して一方向性関数を用いて前記画像ファイルデータに固有のメッセージダイジェスト値を算出する算出処理と、前記メッセージダイジェスト値を前記機器固有の秘密鍵もしくはユーザ定義による秘密鍵により暗号化して署名を得る署名処理と、前記署名をメモリカード内のプロバティ領域に保存するとともに、署名対象の画像ファイルデータをメモリカード内の画像ファイル領域に保存する保存処理とを行うことを特徴としている。

【００１０】本発明の記憶媒体は、前記に記載の各手段を構成するプログラムをコンピュータから読み出し可能に格納したことを特徴としている。また、本発明の他の特徴とするところは、前記に記載の画像形成方法を実行するプログラムをコンピュータから読み出し可能に格納したことを特徴としている。

【００１１】

【発明の実施の形態】以下、本発明のメモリカード、画像形成装置、画像形成方法及び記憶媒体の実施の形態を図面を参照して説明する。

「第１の実施の形態」電子署名技術として現在、ＲＳＡ（Rivest－Shamir－Adelman）方式などのいわゆる非対称公開鍵方式を利用したものがある。前記非対称公開鍵方式は、「公開鍵」と「秘密鍵」という一対の鍵情報を設定している。

【００１２】図１３及び図１４は、前記電子署名について概念的に説明したものである。この技術においては、図１４中の「メッセージダイジェスト値」と「公開鍵」がポイントとなっている。前記メッセージダイジェスト値は、個々のメッセージに対し固有の値を有している。

【００１３】まず、署名したいデータ（テキストやバイナリ）に対して、メッセージダイジェスト値を算出する。前記メッセージダイジェスト値は、一方向性関数（ハッシュ関数）を用いて、署名したいデータから作成されるものであり、署名したいデータに固有の値である。そして、前記のように作成されたメッセージダイジェスト値を秘密鍵で暗号化する。

【００１４】電子的データの送受信を行う場合、送信側は前記秘密鍵で暗号化されたメッセージダイジェスト値を署名として、署名対象データと一緒に受信側に送り出す。受信側は、受信した署名データを署名側の公開鍵で復号化してメッセージダイジェスト値を得る。そして、受信した署名対象データから算出されるメッセージダイジェスト値と、前記復号化したメッセージダイジェスト値とを比較する。前記のような手順で署名の検証を行うことができる。以下、本実施の形態の更に詳細に説明する。図１は、本実施の形態にかかわる画像ファイルデータの改ざん防止機能を備えた画像形成装置の構成を示すブロック図である。この画像装置は、制御装置（ＣＰＵ）４１、メモリ４２、入力装置４３、出力装置４４、メモリカードI/F４５、とからなる。そして、この画像形成装置は状況に応じてネットワークI/F４６、外部記録装置４７をも含むことがある。

【００１５】制御装置４１は、この画像形成装置の各部

の動作を統括して管理するものであり、マイクロプロセッサ及びその周辺回路で構成されている。メモリ４２は、例えばＲＯＭ（Read Only Memory）、ＲＡＭ（Random Access Memory）等があり、この画像形成装置で実行されるプログラム、処理に用いられるデータ、ユーザが作成したデータ等が格納されている。

【００１６】入力装置４３は、例えばキーボード、ポインティングデバイス、タッチパネル等に相当し、制御装置４１に対して各種の動作を指示するために用いられる。出力装置４４は、例えばＣＲＴ、液晶表示装置等に相当し、システムからのメッセージや視覚化されたモデル図などが表示される。

【００１７】メモリカードI/F４５は、メモリカード４８に蓄積されているデータを読みとったり、メモリ４２に蓄積されているデータをメモリカード４８に書き込んだりするものである。

【００１８】外部記録装置４７は、例えば磁気ディスク装置、光ディスク装置、光磁気ディスク装置等であり、上述のプログラムやデータを保存しておき、必要に応じてそれらをメモリ４２にロードして使用することができる。

【００１９】ネットワークI/F４６は、ＬＡＮ、モデム等の任意のネットワーク（回線）を介して外部の装置と通信をする。これにより、必要に応じて前記プログラムや前記データを外部の装置からネットワークを介して受け取り、それらをメモリ４２にロードして使用することができる。

【００２０】一方、図２はメモリカード４８のメモリマップの一例を示す図であり、画像ファイルデータ、画像ファイルデータの署名及びプロパティファイルが保存されている。プロパティファイルは、基本的にＡＳＣＩＩコードのみで使用したＴｅｘｔ形式により記載されており、画像ファイルを印刷したい場合はプリントジョブごとに指定情報が完結する記述となっている。

【００２１】また、プロパティファイルは、メモリカード４８内に１つ存在し、対象となる画像ファイルデータは保存場所を問わない。さらに、本実施の形態においては、どの画像形成装置でも書きこみ可能な通常領域と、アクセス権利の設定を行うことにより、指定された、若しくはアクセス権利の設定を行なった画像形成装置以外による書き込みを禁止するように設定可能なデータ記憶領域を設定し、ユーザの判断で画像ファイルデータや画像ファイルデータの署名などを保存することができるようにしている。

【００２２】次に、前記構成からなる第１の実施の形態に関わる画像ファイルデータの改ざん防止を行うために、画像形成装置に配設されている制御手段の一例について、図１の装置構成ブロック図及び図３のフローチャートを用いて説明する。

【００２３】本実施の形態では、図４に示すように、ＭＤ５と呼ばれるハッシュ関数を用いて署名したいデータのメッセージダイジェスト値を算出するようにしている。ＭＤ５は現在、暗号化プログラムの１つであるＰＧＰ（Pretty Good Privacy）で実際に使われているメッセージダイジェスト関数である。

【００２４】画像形成装置にて、ユーザが作成した画像ファイルデータをメモリカード４８に保存しようとするとき、ユーザは入力装置４３よりその保存処理を指示し、その信号が制御装置４１に入力されることにより制御が開始される。

【００２５】制御装置４１は、そのデータに電子署名を行うかどうかユーザに確認するため、出力装置４４にその意向を表示する（ステップＳ６１）。図５は、この意向表示の一例を示す図であり、これに限定されるものではない。署名を行わない場合は、すぐさまメモリカード４８の通常領域にその画像ファイルデータを保存して制御処理を終了する（ステップＳ６６）。

【００２６】一方、署名を行う場合、署名対象画像ファイルデータのメッセージダイジェスト値を算出し（ステップＳ６２）、前記メッセージダイジェスト値を前記画像形成装置が保有している機器固有の秘密鍵で暗号化し（ステップＳ６３）、この暗号化されたメッセージダイジェスト値を署名としてメモリカード４８の対象装置以外書き込み不可領域に保存する（ステップＳ６４）。尚、この機器固有の秘密鍵と対となる機器固有の公開鍵も画像形成装置に保有されている。

【００２７】最後に、署名対象となった画像ファイルデータをメモリカード４８の対象装置以外書き込み不可領域に保存し（ステップＳ６５）、制御処理を終了する。これらの署名や、署名対象となった画像ファイルデータの保存領域をユーザに選択させるようにしても良い。

【００２８】また、本実施の形態によれば、画像ファイルデータをメモリカードに保存する際に、一方向性関数を用いて前記画像ファイルデータのメッセージダイジェスト値を算出し、秘密鍵を用いて前記メッセージダイジェスト値を署名し、前記画像ファイルデータと一緒に前記メモリカードに保存するようにしたので、前記画像ファイルデータの改ざんを確実に防止することができ、前記画像ファイルデータの信頼性を向上させることができる。

【００２９】「第２の実施の形態」前述した第１の実施の形態では、機器固有の秘密鍵、機器固有の公開鍵を用いて行う電子署名方式について述べたが、この第２の実施の形態では、ユーザが定義した秘密鍵、公開鍵を用いての電子署名を行う方式について説明する。

【００３０】この第２の実施の形態に関わる画像ファイルデータの改ざん防止方法を備えた画像形成装置の制御手順の一例について、図１の装置構成ブロック図、及び図６のフローチャートを用いて説明する。

【００３１】ユーザが作成した画像ファイルデータをメ

モリカード４８に保存しようとするとき、ユーザは入力装置４３よりその保存処理を指示し、その信号制御装置４１に入力されることにより制御が開始される。

【００３２】制御装置４１は、そのデータに電子署名を行うかどうかをユーザに確認するため、出力装置４４側にその意向を表示する（ステップＳ７１）。署名を行わない場合は、すぐさまメモリカード４８の通常領域にその画像ファイルデータを保存して制御処理を終了する。

【００３３】一方、署名を行う場合、制御装置４１はユーザに対して、機器固有の秘密鍵を用いるか、新たにユーザ定義による秘密鍵を作成するか、出力装置４４にその意向を表示する（ステップＳ７２）。

【００３４】図７は、この意向表示の一例を示す図であるが、これに限定されるものではない。ユーザ定義による秘密鍵を作成する場合、制御装置４１はユーザに対して任意の暗証番号を入力してもらい（ステップＳ７３）、入力された暗証番号を基にユーザ定義による秘密鍵を自動的に作成する（ステップＳ７４）。

【００３５】この後、前記ユーザ定義による秘密鍵よりユーザ公開鍵が自動的に生成される（ステップＳ７５）。以降、署名対象画像ファイルデータのメッセージダイジェスト値を算出し（ステップＳ７６）、前記メッセージダイジェスト値を選択された機器固有の秘密鍵もしくはユーザ定義による秘密鍵で暗号化し（ステップＳ７７）、暗号化されたメッセージダイジェスト値を署名としてメモリカード４８の対象装置以外書き込み不可領域に保存する（ステップＳ７８）。

【００３６】最後に、署名対象となった画家ファイルデータをメモリカード４８の対象装置以外書き込み不可領域に保存し（ステップＳ７９）、制御処理を終了する。これにより、機器固有となる秘密鍵、公開鍵以外の秘密鍵、公開鍵を使用することができる。

【００３７】また、本実施の形態によれば、ユーザ定義による秘密鍵を新規に作成して電子署名を施すようにしたので、改ざんされ難い電子署名を行うことができる。

【００３８】また、本実施の形態によれば、署名するために用いる秘密鍵をユーザが作成できることにより、機器固有の秘密鍵、公開鍵以外の秘密鍵、公開鍵を使用することができるので、署名された画像ファイルデータの信頼性をより向上させることができる。前述した第２の実施の形態では、ユーザ定義による秘密鍵を新たに作成することにより、機器固有の秘密鍵以外の秘密鍵を用いて電子署名を施す方法について説明した。この第３の実施の形態では、ユーザ定義による秘密鍵、ユーザ公開鍵が画像形成装置に保存されており、それらを利用する方法について説明する。

【００３９】「第３の実施の形態」この第３の実施の形態に関わる画像ファイルデータの改ざん防止方法を備えた画像形成装置の制御手順の一例について、図１の装置構成ブロック図、及び図８のフローチャートを用いて説明する。

【００４０】ユーザが作成した画像ファイルデータをメモリカード４８に保存しようとするとき、ユーザは入力装置４３よりその保存処理を指示し、その信号制御装置４１に入力されることにより制御が開始される。

【００４１】制御装置４１は、そのデータに電子署名を行うかどうかユーザに確認するため、出力装置４４にその意向を表示する（ステップＳ８０１）。署名を行わない場合は、すぐさまメモリカード４８の通常領域にその画像ファイルデータを保存して制御処理を終了する。

【００４２】一方、署名を行う場合、制御装置４１はユーザに対して、機器固有の秘密鍵を使用するか、機器に保存されているユーザ定義による秘密鍵を使用するか、新たにユーザ定義による秘密鍵を作成するか、出力装置４４にその意向を表示する（ステップＳ８０２）。図９は、この意向表示の一例を示す図であるが、これに限定されるものではない。ユーザ定義による秘密鍵を使用しない場合は、前記第１の実施例に準ずる。

【００４３】新たにユーザ定義による秘密鍵を作成する場合は、前記第２の実施の形態に従って秘密鍵暗証番号の入力を行ない（ステップＳ８０３）、秘密鍵、公開鍵を作成した後、前記秘密鍵、前記公開鍵を外部記録装置４６もしくはメモリ４２に保存する（ステップＳ８０４）。ただし、前記保存された秘密鍵、公開鍵は、ユーザの判断により、外部記録装置４６またはメモリ４２から削除することも可能である。

【００４４】一方、ステップＳ８０２の判定の結果、秘密鍵を新規に作成しない場合にはステップＳ８１３に進み、登録済みの秘密鍵を使用するか否かを判断する。この判定の結果、機器に保存されているユーザ定義による秘密鍵を使用する場合、その秘密鍵に設定されている暗証番号を入力し（ステップＳ８０６）、この秘密鍵が前記ユーザのものであるか否かを検証する（ステップＳ８０７）。ここで、保存されているユーザ定義による秘密鍵が複数ある場合は、どれか１つをユーザに選択させ、その選択された秘密鍵の検証を行う。そして、前記ユーザのものと認証された場合は、前記秘密鍵と対となる公開鍵が外部記憶装置４６またはメモリ４２に存在するか確認し（ステップＳ８０８）、存在しなければ自動的に公開鍵を作成し、外部記憶装置４６またはメモリ４２に保存する（ステップＳ８０５）。

【００４５】そして、ステップＳ８０９では、署名対象画像ファイルデータのメッセージダイジェスト値を算出し、前記メッセージダイジェスト値を前記ユーザ定義による秘密鍵で暗号化し（ステップＳ８１０）、暗号化されたメッセージダイジェスト値を署名としてメモリカード４８に保存する（ステップＳ８１１）。最後に、署名対象となった画像ファイルデータをメモリカード４８に保存し（ステップＳ８１２）、制御処理を終了する。

【００４６】「第４の実施の形態」これまでの実施の形

態では、メモリカード４８に署名対象画像ファイルデータと署名のみを保存していた。この第４の実施の形態では、署名を確認するための公開鍵や秘密鍵を、メモリカード４８に保存する方法、画像形成装置の出力装置４４に表示する方法について説明する。

【００４７】この第４の実施の形態に関わる画像ファイルデータの改ざん防止方法を備えた画像形成装置の制御手順の一例について、図１の装置構成ブロック図、及び図１０のフローチャートを用いて説明する。

【００４８】ユーザが作成した署名対象画像ファイルデータ及び署名をメモリカード４８に保存する手順はこれまでの実施の形態と同様である。この後、制御装置４１は前記画像ファイルに使用した秘密鍵及びその対となる公開鍵をメモリカード４８に保存するか、表示装置に表示するかをユーザに確認するため、出力装置４４にその意向を表示する（ステップＳ９０１）。図１１は、この意向表示の一例であるが、これに限定されるものではない。

【００４９】次に、秘密鍵、公開鍵の保存、表示方法について選択する項目が出力装置側に現れる（ステップＳ９０２）、図１２は、この意向表示の一例であるが、これに限定されるものではない。特に、公開鍵は前記画像ファイルデータと前記署名との検証に用いられるため、何らかの方法で保存しておく必要がある。これらの扱いについては、以下のような選択肢がある。

【００５０】（公開鍵について）

（１）公開鍵を画像ファイルデータと署名が保存されているメモリカード４８と同一のメモリカード４８に保存する。

（２）公開鍵を画像ファイルデータと署名が保存されているメモリカード４８と別のメモリカードに保存する。

（３）公開鍵を出力装置に表示する。

【００５１】（秘密鍵について）

（１）秘密鍵を画像ファイルデータと署名が保存されているメモリカード４８と同一のメモリカードに保存する。

（２）秘密鍵を画像ファイルデータと署名が保存されているメモリカード４８とは別のメモリカードに保存する。

（３）秘密鍵を出力装置に表示する。

【００５２】ステップＳ９０３及びステップＳ９０９の質問に応えて、前記秘密鍵、前記公開鍵の保存・表示方法を選択した後、前記秘密鍵、前記公開鍵を署名付き画像ファイルデータを保存しているメモリカード４８と同一メモリカードに保存する（ステップＳ９０４及びＳ９１０）。

【００５３】また、ステップＳ９１５の質問に応えて前記秘密鍵及び公開鍵を、署名付き画像ファイルデータと別のメモリカードに保存する場合、メモリカード４８を交換するようユーザに指示した後に、交換されたメモリカード４８を認識後、前記秘密鍵及び公開鍵を保存する（ステップＳ９１６及びＳ９１７）。

【００５４】また、ステップＳ９０５の質問に応えて、秘密鍵をデータとは別メモリカードに保存する場合には、ステップＳ９０６において秘密鍵保存フラグをＯＮにする。また、ステップＳ９１１の質問に応えて、公開鍵をデータとは別メモリカードに保存する場合には、ステップＳ９１２において公開鍵保存フラグをＯＮにする。

【００５５】ステップＳ９０７及びステップＳ９１３の質問に応えて前記秘密鍵及び公開鍵を出力装置４４に表示する場合、前記秘密鍵、前記公開鍵を出力装置に表示する（ステップＳ９０８及びステップＳ９１４）。前記秘密鍵、前記公開鍵を保存、及び表示した後、制御装置４１は処理を終了する。これらの秘密鍵や公開鍵は、ユーザの選択によりメモリカード４８の前記画像形成装置以外書き込み不可領域に保存することもできる。

【００５６】また、本実施の形態によれば、ユーザが作成した秘密鍵、公開鍵を画像形成装置に保存することにより、前記秘密鍵、前記公開鍵を再利用する際に、より容易に利用できることができる。

【００５７】また、本実施の形態によれば、署名に用いた秘密鍵やその対となる公開鍵をメモリカードに保存したり前記秘密鍵、前記公開鍵を画像形成装置の出力装置に表示することにより、ユーザは前記秘密鍵、前記公開鍵を保管することができ、検証時に前記公開鍵を容易に用いることができたり、前記秘密鍵を再利用することができる。

【００５８】（本発明の他の実施の形態）本発明は複数の機器（例えば、ホストコンピュータ、インターフェース機器、リーダ、プリンタ等）から構成されるシステムに適用しても１つの機器からなる装置に適用しても良い。

【００５９】また、上述した実施の形態の機能を実現するように各種のデバイスを動作させるように、上記各種デバイスと接続された装置あるいはシステム内のコンピュータに対し、上記実施の形態の機能を実現するためのソフトウェ。のプログラムコードを供給し、そのシステムあるいは装置のコンピュータ（ＣＰＵあるいはＭＰＵ）に格納されたプログラムに従って上記各種デバイスを動作させることによって実施したものも、本発明の範疇に含まれる。

【００６０】また、この場合、上記ソフトウェ。のプログラムコード自体が上述した実施の形態の機能を実現することになり、そのプログラムコード自体、及びそのプログラムコードをコンピュータに供給するための手段、例えばかかるプログラムコードを格納した記憶媒体は本発明を構成する。かかるプログラムコードを記憶する記憶媒体としては、例えばフロッピー（登録商標）ディスク、ハードディスク、光ディスク、光磁気ディスク、Ｃ

D－ＲＯＭ、磁気テープ、不揮発性のメモリカード、ＲＯＭ等を用いることができる。

【００６１】また、コンピュータが供給されたプログラムコードを実行することにより、上述の実施の形態で説明機能が実現されるだけでなく、そのプログラムコードがコンピュータにおいて稼働しているＯＳ（オペレーティングシステム）あるいは他のアプリケーションソフト等の共同して上述の実施の形態で示した機能が実現される場合にもかかるプログラムコードは本発明の実施の形態に含まれることは言うまでもない。

【００６２】さらに、供給されたプログラムコードがコンピュータの機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに格納された後、そのプログラムコードの指示に基づいてその機能拡張ボードや機能拡張ユニットに備わるＣＰＵ等が実際の処理の一部または全部を行い、その処理によって上述した実施の形態の機能が実現される場合にも本発明に含まれる。

【００６３】また、上記各実施の形態によれば、ユーザの選択によりメモリカードの前記画像形成装置以外書き込み不可領域に署名、画像ファイルデータ、秘密鍵、公開鍵を保存することもでき、それらのファイルのセキュリティーを向上させることができる。

【００６４】

【発明の効果】以上説明したように、本発明によれば、画像形成装置で作成してメモリカードに保存されている画像ファイルデータの改ざんを有効に防止することができ、前記画像ファイルデータの信頼性を大幅に向上させることができる。

【図面の簡単な説明】

【図１】画像ファイルデータの改ざん防止機能を備えた画像形成装置の構成例を示すブロック図である。

【図２】メモリカードのメモリマップの一例を示す説明＊

＊図である。

【図３】第１の実施の形態の画像形成装置の処理手順を説明するフローチャートである。

【図４】電子的データとメッセージダイジェスト値との関連を説明する図である。

【図５】第１の実施の形態を説明する画像形成装置の表示部の一例を示す説明図である。

【図６】第２の実施の形態の画像形成装置の処理手順を説明するフローチャートである。

【図７】第２の実施の形態を説明する画像形成装置の表示部の一例を示す説明図である。

【図８】第３の実施の形態の画像形成装置の処理手順を説明するフローチャートである。

【図９】第３の実施の形態を説明する画像形成装置の表示部の一例を示す説明図である。

【図１０】第４の実施の形態を説瞑するフローチャートである。

【図１１】第４の実施の形態を説明する画像形成装置の表示部の一例を示す説明図である。

【図１２】第４の実施の形態を説明する画像形成装置の表示部の一例を示す説明図である。

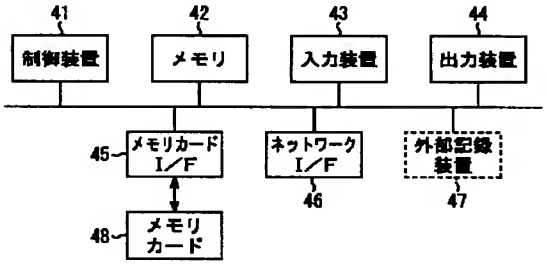
【図１３】電子署名に関する説明図である。

【図１４】電子署名に関する説明図である。

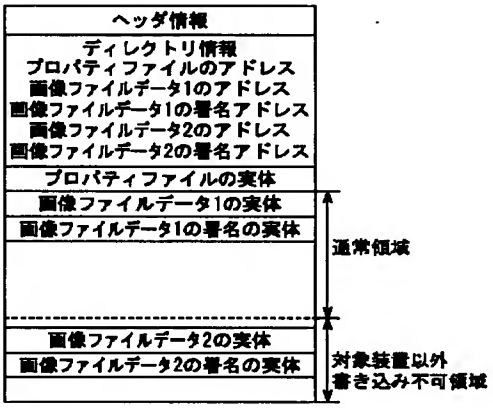
【符号の説明】

４１　制御装置
４２　メモリ
４３　入力装置
４４　出力装置
４５　メモリカードI/F
４６　ネットワークI/F
４７　外部記憶装置
４８　メモリカード

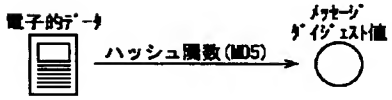
【図１】



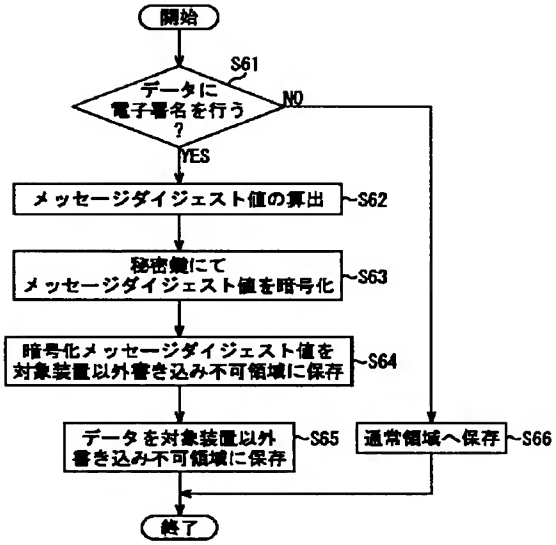
【図２】



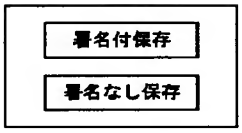
【図４】



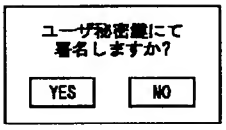
【図３】



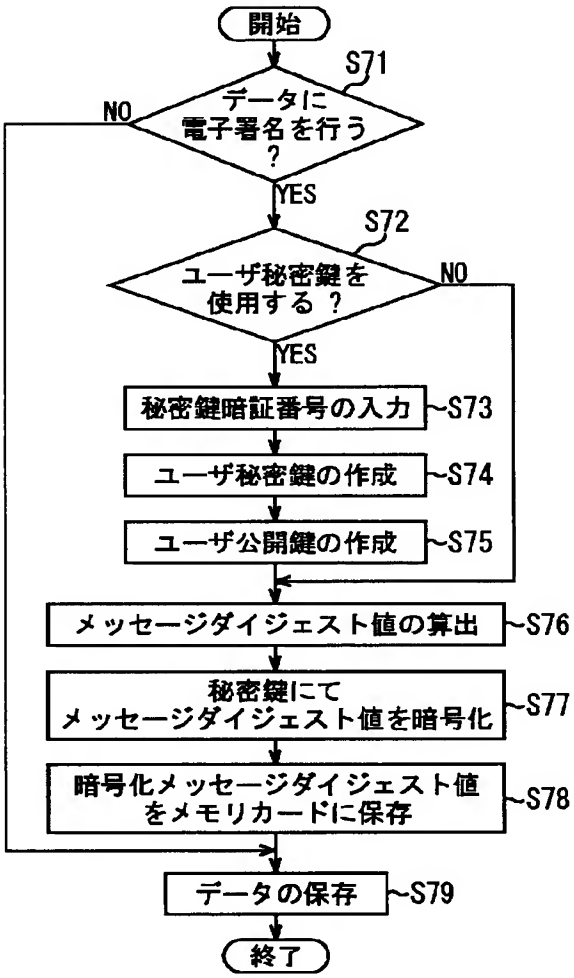
【図５】



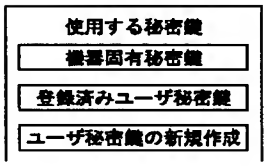
【図７】



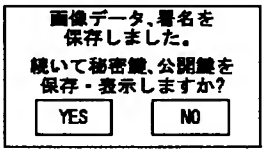
【図６】



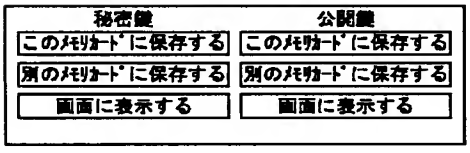
【図９】



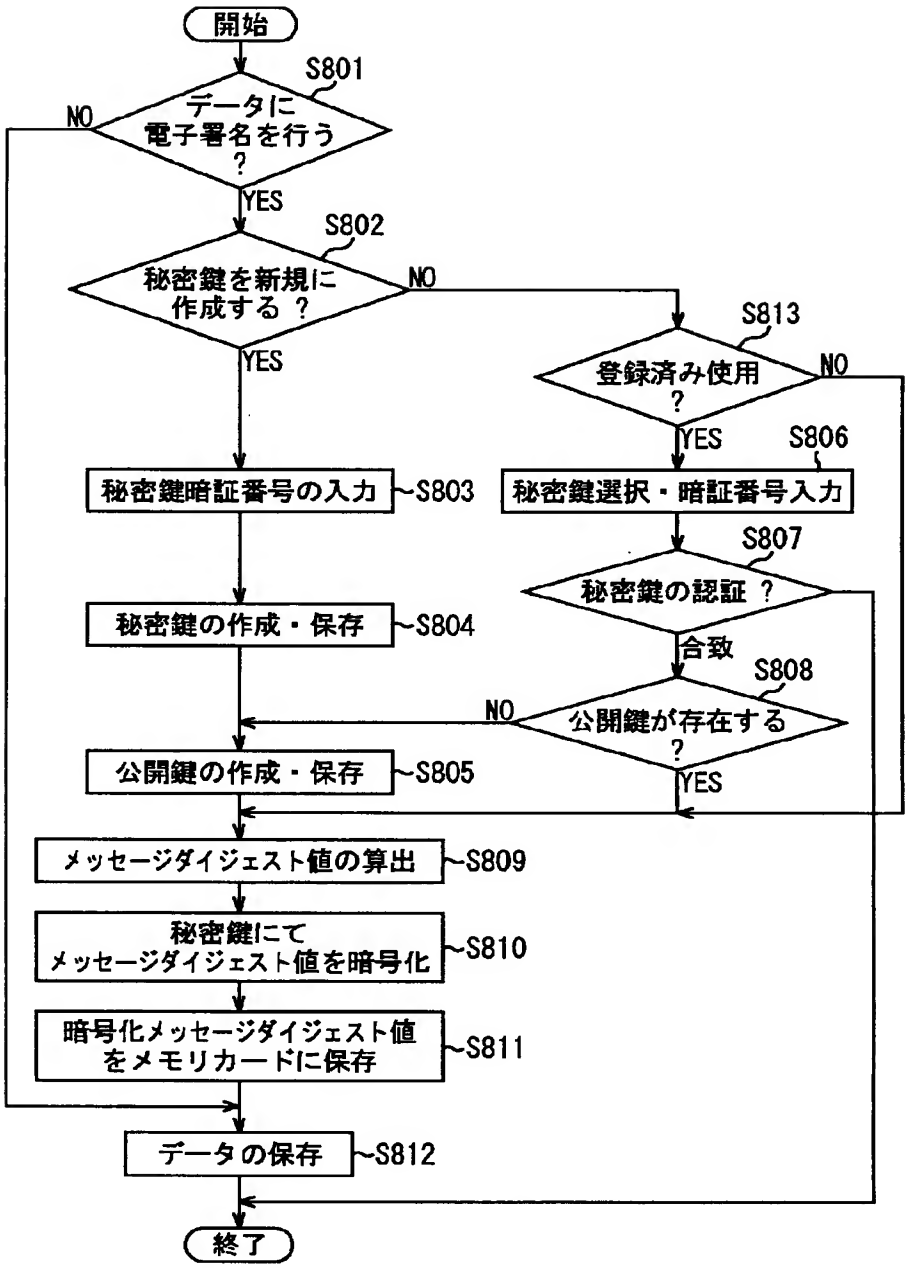
【図１１】



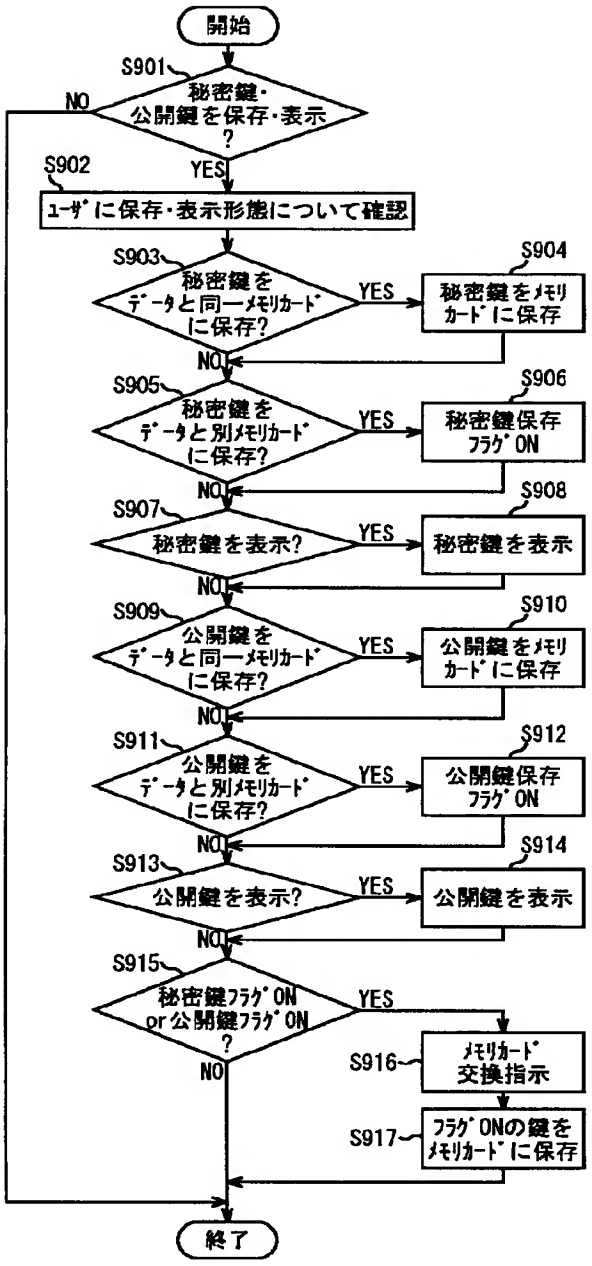
【図１２】



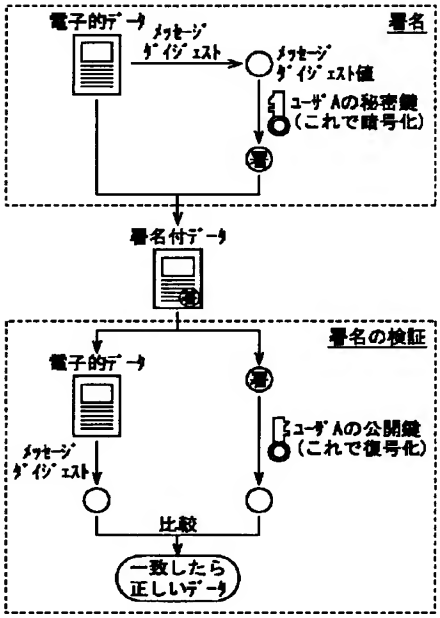
【図８】


開始
S801
データに電子署名を行う？
NO
YES
S802
秘密鍵を新規に作成する？
NO
YES
S813
登録済み使用？
NO
YES
S806
秘密鍵暗証番号の入力
S803
秘密鍵選択・暗証番号入力
S807
秘密鍵の認証？
秘密鍵の作成・保存
S804
合致
S808
NO
公開鍵が存在する？
公開鍵の作成・保存
S805
YES
メッセージダイジェスト値の算出
S809
秘密鍵にてメッセージダイジェスト値を暗号化
S810
暗号化メッセージダイジェスト値をメモリカードに保存
S811
データの保存
S812
終了

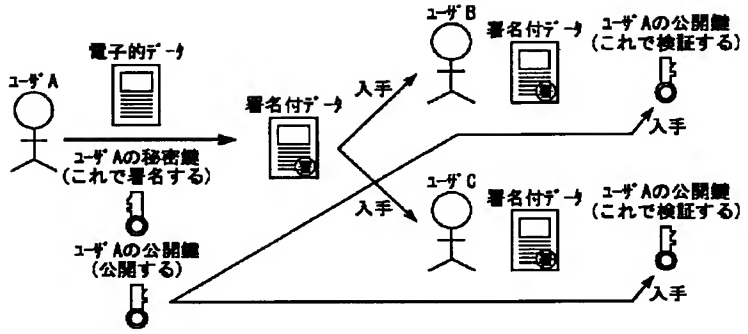
【図１０】


開始
S901
秘密鍵・公開鍵を保存・表示?
NO
YES
S902
ユーザに保存・表示形態について確認
S903
秘密鍵をデータと同一メモリカードに保存?
YES
S904
秘密鍵をメモリカードに保存
NO
S905
秘密鍵をデータと別メモリカードに保存?
YES
S906
秘密鍵保存フラグON
NO
S907
秘密鍵を表示?
YES
S908
秘密鍵を表示
NO
S909
公開鍵をデータと同一メモリカードに保存?
YES
S910
公開鍵をメモリカードに保存
NO
S911
公開鍵をデータと別メモリカードに保存?
YES
S912
公開鍵保存フラグON
NO
S913
公開鍵を表示?
YES
S914
公開鍵を表示
NO
S915
秘密鍵フラグON or公開鍵フラグON ?
YES
S916
メモリカード交換指示
S917
フラグONの鍵をメモリカードに保存
NO
終了

【図１４】


電子的データ
メッセージダイジェスト
メッセージダイジェスト値
ユーザAの秘密鍵(これで暗号化)
署名
署名付データ
署名の検証
電子的データ
メッセージダイジェスト
ユーザAの公開鍵(これで復号化)
比較
一致したら正しいデータ

【図１３】



フロントページの続き

(51)Int.Cl.'	識別記号	Ｆ Ｉ		テーマコード (参考)
// Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７５Ｂ	